Schaumburg Thoenes Thurn Landskron
New PCT Application
Case No. P05,0424 (26970-0398)
Client Ref. No. 2003-0701 PUS
Inventor: Jörgens et al.
Re: Substitute pages

Translation / 19 December 2005 / Bullock / 4780 words

SUBSTITUTE PAGES

In the printing of sensitive data such as, for example, the PIN for check cards or credit cards, a print file that contains the sensitive data is initially created and this file is encrypted. This process occurs in a security zone, i.e. in a hermetically sealed room on a computer system that can be separated from further networks during the operation, such that it is ensured that no unauthorized third parties can access the data to be processed. The print file so created is, for example, transferred onto a printing device with a data medium. The printout in turn occurs in a hermetically sealed room since, in the known printing devices, the encrypted data are decrypted and exist in a readable, decrypted form in the printing device. It is therefore necessary that, during the printing process, only a few authorized persons have access to the device and that the room in which the printing device is located is sealed. However, this also has the consequence that a print job with sensitive print data cannot simply be executed between two print jobs that merely contain non-sensitive data since extensive security measures must be taken for printing of the sensitive data. This applies even when the data are printed on a recording medium given which the printed data cannot be read after the printing process without destroying a casing or a seal or a corresponding other security mechanism. Such recording media are, for example, envelopes with an insert sheet that can be mechanically printed from the outside. Recording media with a security mechanism that makes a reading of sensitive data impossible without detectable alteration of the security mechanism is [sic] designated in the following as safety paper. Furthermore, safety paper is developed that can not just be mechanically printed but can also be printed with an electrophotographic printing device.

US 2002/0032703 A1 discloses a printing in which confidential data are buffered on a fixed disc. After a successful printing of the data, these data on the fixed disc are deleted again, whereby the confidential handling of the data should be assured.

A network system that comprises a printer arises from EP 0 858 021 A2. Confidential print jobs are secured by a PIN. In order that a confidential print job is printed by a printer, a user must input the PIN at the Printer [sic] such that he can ensure that the print copy does not arrive at unauthorized hands.

A similar network system is known from US 5,633,932, in which the print jobs must also be authenticated before the printout.

Since, in the known printing devices, the encrypted data is present in readable form in the printer, it is not possible to execute a print job of such sensitive data without hermetic sealing of the printing device.

A significant requirement exists for a printing device with which sensitive data can be printed without the printing device having to be hermetically sealed for printout of the data.

A printer that is provided for printout of sensitive data arises from US 2002/0184495. This printer comprises a device with which it is determined whether received data to be printed are stored in a volatile or non-volatile memory. If the data should be stored in a non-volatile memory, it is assessed whether they are sensitive data that are then encrypted before they are stored on the non-volatile memory. If the data are stored in the volatile storage medium, an encryption is not necessary since the data are lost given a theft of the printer or, respectively, of the storage medium.

If sensitive data should be printed in large quantities, it is thus appropriate to use an electrophotographic printing device because corresponding high-capacity printers offer a high throughput, whereby every single page can be printed individually. In electrophotographic printers, a character generator is activated by means of a controller, which character generator exposes (with a laser or with light-emitting diodes) a photoconductor drum with which ink particles are

transferred onto a recording medium. In "Das Druckerbuch – Technik und Technologien der OPS-Hochleistungsdrucker [sic], edition 5a, October 2000, ISBN-3-00-001019-X, such optical character generators are described in chapter 4 and a corresponding controller (the SRA controller) for activation of character generators is described in chapter 9. Raster techniques and their effect on the print quality are explained in chapter 6.

The invention is based on the object to achieve a method for printing of sensitive data given whose execution on a printing device it is not necessary to hermetically seal this printing device. Additionally, a device for execution of this method should be achieved with the invention.

The object is achieved via a method with the features of the claim 1 and via a device with the features of the claim 17. Advantageous embodiments of the invention are specified in the respective sub-claims.

The inventive method for printing of sensitive data comprises the following steps:

- encryption at a workstation of sensitive data to be printed,
- transfer to a printing device of the data to be printed,
- decryption of the sensitive data to be printed,

Claims

1. Method for printing of sensitive data, comprising the following steps:
   - encryption at a workstation (2) of sensitive data to be printed,
   - transfer to a printing device (1) of the data to be printed,
   - decryption of the sensitive data to be printed,
   - conversion of the data to be printed into control signals for activation of a printing unit (9, 10, 11),
   - printing of the data on a recording medium,

   whereby the decrypted data are not stored in a readable format on a non-volatile storage medium between the decryption and the printing of the data, in that the decrypted data or, respectively, the control signals containing sensnitive [sic] data are stored in a non-volatile memory, whereby the data are distributed on a plurality of memory segments and their association is stored independent of the data.

2. Method according to claim 1,
characterized in that
the decrypted data are stored in a volatile memory such as, for example, RAM between the decryption and the printing.

3. Method according to claim 1,
characterized in that
the association of the memory segments is stored in a volatile memory (RAM).

4. Method according to any of the claims 1 through 3,
characterized in that
the control signals containing sensitive data are stored in a volatile memory such as, for example, RAM.

5. Method according to any of the claims 1 through 4, characterized in that the decryption and the conversion into control signals is [sic] executed in immediate temporal succession.

6. Method according to any of the claims 1 through 4, characterized in that the decryption and the conversion into control signals is executed in a controller (12) for activation of a character generator (10).

7. Method according to any of the claims 1 through 6, characterized in that the data to be printed are transferred to the printing device in the form of a print data stream such as, for example, IPDS, PDF, PCL or PS, the print data stream is converted into an intermediate language in the printing device, and the print data are decrypted and converted into control signals.

8. Method according to any of the claims 1 through 7, characterized in that the print data contain both sensitive data and non-sensitive data.

9. Method according to claim 8, characterized in that the sensitive data and the non-sensitive data are connected into one data unit (such as, for example, a print file) before the transfer to the printing device.

10. Method according to claim 9, characterized in that

the sensitive data are identified in the data unit via markings.

11. Method according to claim 9 or 10,
characterized in that
a layout that comprises regions to receive sensitive data is generated using the non-sensitive data.

12. Method according to any of the claims 9 through 10 [sic],
characterized in that
the sensitive data are already encrypted before the combination with the non-sensitive data into one data unit.

13. Method according to any of the claims 9 through 10,
characterized in that
the sensitive data are encrypted after the combination with the non-sensitive data into one data unit.

14. Method according to claim 13,
characterized in that
only the sensitive data are encrypted.

15. Method according to claim 13,
characterized in that
both the sensitive data and the non-sensitive data are encrypted.

16. Method according to any of the claims 1 through 15,
characterized in that
the conversion of the data to be printed into control signals for activation of a printing unit via rastering of the data to be printed into one or more raster images is excuted [sic], whereby the raster images represent the control signals.

17. Device for printing of sensitive data according to the method according to any of the claims 1 through 16, with

- a printing unit (9, 10, 11)
- a controller (12) for activation of the printing unit,

whereby the controller (12) is fashioned to receive a print data stream that can contain encrypted data, and that [sic] the sensitive data are decrypted and converted into control signals for activation of the printing unit, whereby the decrypted data are not stored in a readable format on a non-volatile storage medium, in that the decrypted data or, respectively, the control signals containing sensnitive [sic] data are stored in a non-volatile memory, whereby the data are distributed on a plurality of memory segments and their association is stored independent of the data.

18. Device according to claim 17,
characterized in that
the printing unit comprises a character generator (10).

19. Device according to claim 17 or 18,
characterized in that
the device is an electrophotographic high-capacity printer.

20. Device according to any of the claims 17 through 19,
characterized in that
the controller (12) comprises a decryption module (16) and one or more raster modules (17).

21. Device according to any of the claims 17 through 19,
characterized in that

the controller (12) comprises a combined decryption/raster module.

22. Device according to any of the claims 17 through 21, characterized in that the controller (12) comprises only volatile storage media.

23. Device according to any of the claims 17 through 22, characterized in that a sensor for detection of recording media with predetermined security features is arranged on a transport path (6) for recording media in the region before the printing unit (9, 10, 11), such that the printing of sensitive data can be stopped given the detection of recording media without security features.